

U 9/890286

28.01.00

JP00 / 475  
日 本 国 特 許 庁PATENT OFFICE  
JAPANESE GOVERNMENT

REC'D 17 MAR 2000

WIPC PCT

Best Available Copy

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。 #3

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application:

1999年 8月26日

出 願 番 号  
Application Number:

平成11年特許願第239177号

出 願 人  
Applicant(s):

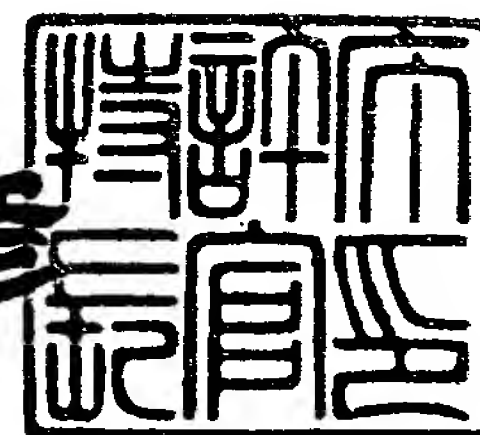
株式会社日立製作所

PRIORITY  
DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH RULE 17.1(a) OR (b)

2000年 3月 3日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



出証番号 出証特2000-3011680

【書類名】 特許願

【整理番号】 K99009761

【提出日】 平成11年 8月26日

【特記事項】 特許法第 3 0 条第 1 項の規定の適用を受けようとする特  
許出願

【あて先】 特許庁長官殿

【国際特許分類】 G09C 1/00

【請求項の数】 17

【発明者】

【住所又は居所】 神奈川県川崎市麻生区王禅寺 1 0 9 9 番地 株式会社日  
立製作所 システム開発研究所内

【氏名】 西岡 玄次

【特許出願人】

【識別番号】 000005108

【氏名又は名称】 株式会社日立製作所

【代理人】

【識別番号】 100075096

【弁理士】

【氏名又は名称】 作田 康夫

【手数料の表示】

【予納台帳番号】 013088

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 選択暗号文攻撃に強い公開鍵暗号方法及び装置

【特許請求の範囲】

【請求項 1】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数 1】

- $G$  : 有限アーベル群
  - $s \in \mathbb{Z}, gh^s = 1 \ (\in H)$
  - $\alpha^{-1} \in \mathbb{Z}$
- ... (数1)

なる秘密鍵  $(G, s, \alpha^{-1})$  を作成し (但し,  $\alpha^{-1}$  は  $H$  の濃度を法とする環における  $\alpha$  の逆元), さらに、

【数 2】

- $H : G$  の部分群
  - $g, h \in G$
  - $\alpha \in \mathbb{Z}$
- ... (数2)

なる公開鍵  $(H, g, h, \alpha)$  を作成し (但し,  $k$  は  $pq$  のビット長),

(1) 送信者は、平文  $m (\in H)$  および乱数  $r$  に対して、

【数 3】

$$C = m^\alpha g^r, \quad D = h^r \quad (\in G) \quad \dots (数3)$$

を計算し、さらに暗号文から平文が一意的に復号化されるための付加情報  $a$  を計算し、 $(C, D, a)$  を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の秘密鍵  $(H, s, \alpha^{-1})$  を用いて、暗号文  $(C, D, a)$  から

【数 4】

$$\hat{m} = (CD^e)^{\alpha^{-1}} \quad (\in H) \quad \cdots (数4)$$

を計算し、さらに付加情報aから元の平文mを計算することを特徴とする公開鍵暗号方法。

【請求項 2】

請求項 1 において、前記公開情報 (G, g, h, α) は、前記受信者が生成し、公開することを特徴とする公開鍵暗号方法。

【請求項 3】

請求項 1 および 2 において、

ランダム関数 H を公開するステップを備え、

送信者が作成した平文に対して、乱数情報とランダム関数 H の結果を排他的論理和およびデータの接続による演算を行うステップを備え、

さらに、該演算を行った結果を、請求項 1 における平文 m の箇所、または、乱数 r の箇所に置き換え、請求項 1 における公開鍵暗号化方法の手順により暗号化する

ことを特徴とする公開鍵暗号における暗号化方法。

【請求項 4】

請求項 3 の方法により暗号化した暗号文を復号化する方法において、

請求項 1 の公開鍵暗号方法による復号化手順を行うステップを備え、

さらに、請求項 3 において行われた該演算（平文 m' に対して乱数情報とランダム関数 H の結果を排他的論理和およびデータの接続による演算）の手順の正当性を確かめるステップを備え、

その後、復号化結果を出力する

ことを特徴とする公開鍵暗号における復号化方法。

【請求項 5】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数 5】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  . . . (数5)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵  $(p, q, s, \beta)$  を作成し, さらに,

【数 6】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  . . . (数6)
- $n = p^d q \quad (d \text{ は奇数})$

なる公開鍵  $(n, g, h, k, l, \alpha)$  を作成し (但し,  $k$  は  $pq$  のビット長),

(1) 送信者は, 平文  $m (0 < m < 2^{k-2})$  および乱数  $r (0 \leq r \leq 1)$  に対して,

【数 7】

$$C = m^{2\alpha} g^{r'} \pmod{n}, \quad D = h^{r'} \pmod{n} \quad \dots \text{(数7)}$$

を計算し, さらに Jacobi 記号  $a = (m/n)$  を計算し,  $(C, D, a)$  を暗号文として前記受信者に送信し,

(2) 前記受信者は, 自身の秘密鍵  $(p, q, s, \beta)$  を用いて, 暗号文  $(C, D, a)$  から

【数 8】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{s(p+1)}{4}} \pmod{p}, \\ m_{1,q} &= (CD^s)^{\frac{s(q+1)}{4}} \pmod{q} \end{aligned} \quad \dots \text{(数8)}$$

を計算し,  $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$  のうち,  $(x/n) = a$  かつ  $0 < x < 2^{k-2}$  を満たす  $x$  を平文  $m$  とする (但し,  $\phi$  は中国人の剰余定理による  $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$  から  $\mathbb{Z}/(pq)$  への環同型写像を表す。),

ことを特徴とする公開鍵暗号方法。

【請求項 6】

請求項 5 において、前記公開情報  $(n, g, h, k, l, \alpha)$  は、前記受信者が生成し、公開することを特徴とする公開鍵暗号方法。

【請求項 7】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数 9】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$  . . . (数 9)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵  $(p, q, \beta)$  を作成し、さらに、

【数 10】

- $\alpha, k \in \mathbb{Z}$  . . . (数 10)
- $n = p^d q$  ( $d$  は奇数)

なる公開鍵  $(n, k, \alpha)$  を作成し (但し、 $k$  は  $pq$  のビット長) ,

(1) 送信者は、平文  $m$  ( $0 < m < 2^{n-k-1}$ ) に対して、

【数 11】

$$m_1 = m0^{k_1} \oplus G(r) \parallel r \oplus H(m0^{k_1} \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \quad \dots \text{(数 11)}$$

を計算し (但し、 $G: \{0, 1\}^{k_0} \rightarrow \{0, 1\}^n$ ,  $H: \{0, 1\}^n \rightarrow \{0, 1\}^{k_0}$ , は適当なランダム関数であり、 $k = n + k_0 + 2$  とする。), さらに Jacobi 記号  $a = (m_1/n)$ , および、

【数 12】

$$C = m_1^{2\alpha} \bmod n, \quad \dots \text{(数 12)}$$

を計算し、 $(C, a)$  を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の秘密鍵  $(p, q, \beta)$  を用いて、暗号文  $(C, a)$  から、

【数 1 3】

$$\begin{aligned} m_{1,p} &= C^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= C^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (数 1 3)$$

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$  のうち、 $(x/n)=a$  かつ  $0 < x < 2^{k-2}$  を満たす  $x$  を  $m'_1$  として計算し（但し、 $\phi$  は中国人の剰余定理による  $Z/(p) \times Z/(q)$  から  $Z/(pq)$  への環同型写像を表す。）、

さらに、 $m'_1 = s' || t'$  ( $s'$  は  $m'_1$  の上位  $n$  ビット、 $t'$  は下位  $k_0$  ビット) に対して、

【数 1 4】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \dots (数 1 4)$$

を計算し、これを復号化結果とする（但し、 $[a]^n$  および  $[a]_n$  はそれぞれ  $a$  の上位および下位  $n$  ビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項 8】

請求項 7 において、前記公開情報  $(n, k, \alpha)$  は、前記受信者が生成し、公開することを特徴とする公開鍵暗号方法。

【請求項 9】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数 1 5】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq} \quad \dots (数 1 5)$
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵  $(p, q, s, \beta)$  を作成し、さらに、

【数 1 6】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n) \quad \dots (数16)$
- $n = p^d q \quad (d \text{ は奇数})$

なる公開鍵  $(n, g, h, k, l, \alpha)$  を作成し (但し,  $k$  は  $pq$  のビット長),

(1) 送信者は, 平文  $m$  ( $0 < m < 2^{n-k-1}$ ) に対して,

【数 1 7】

$$m_1 = m0^{k_1} \oplus G(r) \parallel r \oplus H(m0^{k_1} \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \quad \dots (数17)$$

を計算し (但し,  $G: \{0,1\}^{k_0} \rightarrow \{0,1\}^n$ ,  $H: \{0,1\}^n \rightarrow \{0,1\}^{k_0}$ , は適当なランダム関数であり,  $k=n+k_0+2$  とする。), さらに Jacobi 記号  $a=(m_1/n)$ , および,

【数 1 8】

$$C = m_1^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \quad \dots (数18)$$

を計算し,  $(C, D, a)$  を暗号文として前記受信者に送信し,

(2) 前記受信者は, 自身の秘密鍵  $(p, q, s, \beta)$  を用いて, 暗号文  $(C, D, a)$  から

【数 1 9】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (数19)$$

を計算し,  $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$  のうち,  $(x/n)=a$  かつ  $0 < x < 2^{k-2}$  を満たす  $x$  を  $m'_1$  として計算し (但し,  $\phi$  は中国人の剰余定理による  $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$  から  $\mathbb{Z}/(pq)$  への環同型写像を表す。),

さらに,  $m'_1 = s' \parallel t'$  ( $s'$  は  $m'_1$  の上位  $n$  ビット,  $t'$  は下位  $k_0$  ビット) に対して,



【数 2 0】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \dots (数 2 0)$$

を計算し、これを復号化結果とする（但し、 $[a]^n$ および $[a]_n$ はそれぞれ $a$ の上位および下位 $n$ ビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項 1 0】

請求項 9 において、前記公開情報  $(n, g, h, k, \alpha)$  は、前記受信者が生成し、公開することを特徴とする公開鍵暗号方法。

【請求項 1 1】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数 2 1】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  ... (数 2 1)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵  $(p, q, s, \beta)$  を作成し、さらに、

【数 2 2】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  ... (数 2 2)
- $n = p^d q \quad (d \text{ は奇数})$

なる公開鍵  $(n, g, h, k, l, \alpha)$  を作成し（但し、 $k$ は $pq$ のビット長）、

(1) 送信者は、平文 $m$  ( $0 < m < 2^n$ ) に対して、

【数 2 3】

$$m_1 = m \oplus G(r) \parallel r \oplus H(m \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \quad \dots (数 2 3)$$

を計算し（但し、 $G: \{0,1\}^{k_0} \rightarrow \{0,1\}^n$ ,  $H: \{0,1\}^n \rightarrow \{0,1\}^{k_0}$ , は適当なランダム関数であり、 $k=n+k_0+2$ とする。）、さらにJacobi記号 $a=(m_1/n)$ , および、

【数 2 4】

$$C = m_1^{2a} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \quad \dots (数 2 4)$$

を計算し（但し、 $F: \{0,1\}^{n+k_0} \rightarrow \{0,1\}^l$ は適当なランダム関数）、 $(C,D,a)$ を暗号文として前記受信者に送信し、

（2）前記受信者は、自身の秘密鍵 $(p,q,s,\beta)$ を用いて、暗号文 $(C,D,a)$ から、

【数 2 5】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (数 2 5)$$

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を $m'_1$ として計算し（但し、 $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。）、

さらに、 $m'_1 = s' \parallel t'$ （ $s'$ は $m'_1$ の上位 $n$ ビット、 $t'$ は下位 $k_0$ ビット）に対して、

【数 2 6】

$$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C, D) = (C', D') \\ * & \text{otherwise} \end{cases} \quad \dots (数 2 6)$$

を計算し、これを復号化結果とする（但し、

【数 2 7】

$$C' = m_1'^2 g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n \quad \dots (数 2 7)$$

であり、 $[a]^n$  および  $[a]_n$  はそれぞれ  $a$  の上位および下位  $n$  ビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項 1 2】

請求項 1 1 において、前記公開情報  $(n, g, h, k, \alpha)$  は、前記受信者が生成し、公開することを特徴とする公開鍵暗号方法。

【請求項 1 3】

送信者は、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【数 2 8】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  ... (数 2 8)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

なる秘密鍵  $(p, q, s, \beta)$  を作成し、さらに、

【数 2 9】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  ... (数 2 9)
- $n = p^d q \quad (d \text{ は奇数})$

なる公開鍵  $(n, g, h, k, l, \alpha)$  を作成し（但し、 $k$  は  $pq$  のビット長）、

(1) 送信者は、平文  $m$  ( $0 < m < 2^n$ ) に対して、乱数  $r$  ( $0 < r < 2^{k_0}$ ) を選び、

【数 3 0】

$$m_1 = m \parallel r \quad \dots (\text{数} 3 0)$$

を計算し（但し、 $F: \{0,1\}^{n+k_0} \rightarrow \{0,1\}^1$  は適当なランダム関数であり、 $k=n+k_0+2$  とする。）、さらにJacobi記号 $a=(m_1/n)$ 、および、

【数 3 1】

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \quad \dots (\text{数} 3 1)$$

を計算し、 $(C,D,a)$ を暗号文として前記受信者に送信し、

（2）前記受信者は、自身の秘密鍵 $(p,q,s,\beta)$ を用いて、暗号文 $(C,D,a)$ から

【数 3 2】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (\text{数} 3 2)$$

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を $m'_1$ として計算し（但し、 $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。）、

さらに、

【数 3 3】

$$m' = \begin{cases} [m'_1]^{k_0} & \text{if } (C,D) = (C',D') \\ * & \text{otherwise} \end{cases} \quad \dots (\text{数} 3 3)$$

を計算し、これを復号化結果とする（但し、

【数 3 4】

$$C' = m_1'^2 g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n \quad \dots (数 3 4)$$

であり、 $[a]^n$  および  $[a]_n$  はそれぞれ  $a$  の上位および下位  $n$  ビットを表す。）

ことを特徴とする公開鍵暗号方法。

【請求項 1 4】

請求項 1 3 において、前記公開情報  $(n, g, h, k, \alpha)$  は、前記受信者が生成し、公開することを特徴とする公開鍵暗号方法。

【請求項 1 5】

請求項 7 から請求項 1 4 において、  
 $d$  ( $d \geq 1$ ) の値を可変とする  
 ことを特徴とする公開鍵暗号方法および鍵共有方法。

【請求項 1 6】

請求項 9 および請求項 1 0 において、暗号化処理のとき、

【数 3 5】

$$g^{r'} \bmod n, \quad h^{r'} \bmod n \quad \dots (数 3 5)$$

の計算を前処理にて行うステップを備える

ことを特徴とする公開鍵暗号方法。

【請求項 1 7】

請求項 1 1 から請求項 1 4 において、復号化処理のとき、  
 受信者側は、

【数 3 6】

$$\begin{aligned} C'_p &= m_1'^{2\alpha} g^{F(m_1')} \bmod p^d, & C'_q &= m_1'^2 g^{F(m_1')} \bmod q \\ D'_p &= h^{F(m_1')} \bmod p^d, & D'_q &= h^{F(m_1')} \bmod q \end{aligned} \quad \dots (数 3 6)$$

を計算し、さらに

【数 3 7】

$$\begin{aligned} C &\equiv C'_p \pmod{p^d}, & C &\equiv C'_q \pmod{q}, \\ D &\equiv D'_p \pmod{p^d}, & D &\equiv D'_q \pmod{q} \end{aligned} \quad \dots (\text{数 } 37)$$

により,  $(C,D)=(C',D')$  を検査するステップを備える  
ことを特徴とする公開鍵暗号方法。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

本発明は、公開鍵暗号を用いた暗号通信方法および装置に関する。

【0 0 0 2】

【従来の技術】

現在まで、様々な公開鍵暗号方式が提案されている。なかでも、文献 1 「R.L. Rivest, A. Shamir, L. Adleman.: A method for obtaining digital signatures and public-key cryptosystems, Commun. of the ACM, Vol.21, No.2, pp.120-126, 1987.」に掲載されている方法が最も有名であり、最も実用化されている公開鍵暗号である。

【0 0 0 3】

その他には、文献 2 「T. ElGamal.: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms, IEEE Trans. On Information Theory, IT-31, 4, pp.469-472(1985)」に記載されている暗号方法、文献 3 「M.O. Rabin.: Digital Signatures and Public-Key Encryptions as Intractable as Factorization, MIT, Technical Report, MIT/LCS/TR-212 (1979)」に記載されている暗号方法、文献 4 「V.S. Miller.: Use of Elliptic Curves in Cryptography, Proc. of Crypto'85, LNCS 218, Springer-Verlag, pp.417-426 (1985)」, 文献 5 「N. Koblitz.: Elliptic Curve Cryptosystems, Math. Comp., 48, 177, pp.203-209 (1987)」等に記載の楕円曲線を用いた方法、文献 6 「S. Goldwasser and S. Micali.: Probabilistic Encryption, JCSS, 28, 2, pp.270-299 (1984)」に

記載されている暗号方法, 文献 7 「M.Blum and S.Goldwasser.: An Efficient probabilistic public-key encryption scheme which hides all partial information, Proc. of Crypto'84, LNCS 196, Springer-Verlag, pp.289-299 (1985)」に記載されている暗号方法, 文献 8 「S.Goldwasser and M.Bellare.: Lecture Notes on Cryptography, <http://www-cse.ucsd.edu/users/mihir/> (1997)」に記載されている暗号方法, 文献 9 「R.Cramer and V.Shoup.: A Practical Public Key Cryptosystem Provably Secure against Adaptive Chosen Ciphertext Attack, Proc. of Crypto98, LNCS, Springer-Verlag, pp.13-25 (1998)」に記載されている暗号方法, 文献 10 「T.Okamoto and S.Uchiyama,.A New Public-Key Cryptosystem as Secure as Factoring, Proc. of Eurocrypt'98, LNCS, Springer Verlag, pp.308-318 (1998)」に記載されている暗号方法, などが知られている。

#### 【 0 0 0 4 】

特に, 最近では, 安全性の証明が可能な公開鍵暗号が注目されている。ここで, 安全性が証明できるとは, 「ある攻撃 (受動的攻撃または能動的攻撃) に対してその公開鍵暗号が安全 (強秘匿性, 頑強性, 等) であること」と, 「ある数論的問題 (素因数分解問題, Diffie-Hellman決定問題, 等) が困難であること」の等価性を証明できる公開鍵暗号のことである。

#### 【 0 0 0 5 】

Bellareらは, 文献 11 「M.Bellare, A.Desai, D.Pointcheval and P.Rogaway ,.Relations Among Notions of Security for Public-Key Encryption Schemes, Proc. of Crypto'98, LNCS, Springer Verlag」で, IND-CCA2 (適応的選択暗号文攻撃に対して強秘匿であること) とNM-CCA2 (適応的選択暗号文攻撃に対して頑強であること) の等価性を示し, この条件を満たす公開鍵暗号が最も安全であると考えられている。

#### 【 0 0 0 6 】

例えば, Bellareらは, 文献 12 「M.Bellare and P.Rogaway,.Optimal Asymmetric Encryption How to Encrypt with RSA, Proc. of Eurocrypt'94, LNCS, Springer Verlag」で, 一般的な落とし戸付き置換をIND-CCA2に変換する方法につ

いて提案し、さらにRSA暗号をこの方法により変換した公開鍵暗号方式(OAEP)を提案している。OAEPはランダムオラクルモデル(理想的なランダム関数へのアクセスが許される)の上で安全性が証明でき、実用のシステムではこの部分が適当なハッシュ関数に置き換えられるため、実用のシステムにおいては安全性は証明できないことになる。しかし、同様の安全性を得られるものと予想され、また、同じくIND-CCA2であることが証明されている上記文献9の方法(この方法は理想的なランダム関数を前提としない)等に比べ、効率性が優れる等の特徴を持つ。

#### 【0007】

##### 【発明が解決しようとする課題】

上記「従来の技術」で述べたように、現在では、IND-CCA2(適応的選択暗号文攻撃に対して強秘匿)またはNM-CCA2(適応的選択暗号文攻撃に対して頑強)である公開鍵暗号が最も安全であると考えられている。

#### 【0008】

本発明の目的は、選択平文攻撃に対して一方向(OW-CPA)であり、かつ選択平文攻撃に対して強秘匿(IND-CPA)である公開鍵暗号方法を提供することである。

#### 【0009】

本発明の更なる目的は、従来技術であるOAEPなどに比べて、より困難な問題の計算量的複雑さを前提としてIND-CCA2(またはNM-CCA2)であることが証明できる公開鍵暗号方法を提供することである。

#### 【0010】

また、本発明の他の目的は、送信データを暗号化する際の計算および暗号化データを復号化する際の計算の負荷が小さく、携帯型情報処理機器など計算能力が限られた装置であっても高速処理が可能な、公開鍵を用いた暗号化方法と復号化方法と、それを用いた鍵配送方法や鍵共有方法、さらには、これらの方法を実行するプログラム、装置またはシステムを提供することである。



【0 0 1 1】

【課題を解決するための手段】

上記目的を達成するため、本発明は以下のように構成する。

【0 0 1 2】

(1) 選択平文攻撃に対する一方向性 (OW-CPA) を素因数分解問題よりも困難な問題の難しさを前提として保証可能な公開鍵暗号方法に対して、平文に乱数情報と (理想的) ランダム関数へのアクセスの結果から排他的論理和および接続 (データの単純な接続) の変換 (以下、変換Conと呼ぶ) を行う。これにより、適応的選択暗号文攻撃に対する強秘匿性 (IND-CCA2) を、素因数分解問題の困難性以上の暗号学的仮定により保証する。すなわち、本発明が提供する暗号化方法への安全性を、従来方式よりもさらに高い立場にて保証する。

【0 0 1 3】

これにより、適応的選択暗号文攻撃に対する強秘匿性 (IND-CCA2) を、素因数分解問題の困難性 (または、それ以上) の暗号学的仮定により保証することができる。すなわち、本発明が提供する暗号化方法への安全性を、従来方式よりもさらに高い立場にて保証する。

【0 0 1 4】

(2) 変換Conにおいては、排他的論理和と接続の組み合わせからなる。変換Conは高速な処理が可能であり、変換Conを行った後の本発明による公開鍵暗号方法は変換を行う前の公開鍵暗号方法における高速な暗復号化処理とほぼ同等の処理が可能となる。

【0 0 1 5】

(3) 暗号化の過程において、確率的な情報を用いた処理を施す。これにより、暗号化する平文に対して確率的情報を挿入する必要がない。すなわち、本発明が提供する暗号化方法は、同一の平文であっても暗号文の値が変化する確率暗号である。

【0 0 1 6】

(4) 送信データを暗号化する際の計算および暗号化データを復号化する際の計算の双方の負荷が少なく、高速な暗復号化処理が可能であるように構成する。

【 0 0 1 7 】

すなわち、本発明は、送信者が、受信者の公開鍵を用いて送信データを暗号化する公開鍵暗号方法であって、

鍵生成のステップとして、

【 0 0 1 8 】

【数 3 8】

- $G$  : 有限アーベル群
- $s \in \mathbb{Z}, gh^s = 1 \ (\in H)$  ... (数 3 8)
- $\alpha^{-1} \in \mathbb{Z}$

【 0 0 1 9 】

なる秘密鍵  $(G, s, \alpha^{-1})$  を作成し (但し,  $\alpha^{-1}$  は  $H$  の濃度を法とする環における  $\alpha$  の逆元), さらに、

【 0 0 2 0 】

【数 3 9】

- $H : G$  の部分群
- $g, h \in G$  ... (数 3 9)
- $\alpha \in \mathbb{Z}$

【 0 0 2 1 】

なる公開鍵  $(H, g, h, \alpha)$  を作成し (但し,  $k$  は  $pq$  のビット長),

(1) 送信者は、平文  $m (\in H)$  および乱数  $r$  に対して、

【 0 0 2 2 】

【数 4 0】

$$C = m^\alpha g^r, \quad D = h^r \quad (\in G) \quad \dots (数 4 0)$$

【 0 0 2 3 】

を計算し、さらに暗号文から平文が一意的に復号化されるための付加情報 $a$ を計算し、 $(C,D,a)$ を暗号文として前記受信者に送信し、

(2) 前記受信者は、自身の秘密鍵  $(H,s,\alpha^{-1})$  を用いて、暗号文  $(C,D,a)$  から

【 0 0 2 4 】

【数 4 1】

$$\bar{m} = (CD^s)^{\alpha^{-1}} \quad (\in H) \quad \cdots \text{(数41)}$$

【 0 0 2 5 】

を計算し、さらに付加情報 $a$ から元の平文 $m$ を計算することを特徴とするものである。

【 0 0 2 6 】

本発明の公開鍵暗号方法は、さらに、前記公開情報  $(G,g,h,\alpha)$  は、前記受信者が生成し、公開することを特徴とするものである。

【 0 0 2 7 】

本発明の公開鍵暗号方法は、さらに、ランダム関数 $H$ を公開するステップを備え、

送信者が作成した平文に対して、乱数情報とランダム関数 $H$ の結果を排他的論理和およびデータの接続による演算を行うステップを備え、

さらに、該演算を行った結果を、上記公開鍵暗号化方法における平文 $m$ の箇所、または、乱数 $r$ の箇所に置き換え、上記公開鍵暗号化方法の手順により暗号化することを特徴とするものである。

【 0 0 2 8 】

本発明は、さらに、上記公開鍵暗号方法により暗号化した暗号文を復号化する方法において、

さらに、上記公開鍵暗号方法において行われた該演算（平文 $m'$ に対して乱数情報とランダム関数 $H$ の結果を排他的論理和およびデータの接続による演算）の手順の正当性を確かめるステップを備え、

その後、復号化結果を出力することを特徴とするものである。

【0 0 2 9】

より具体的には、

[鍵生成]

【0 0 3 0】

【数 4 2】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  ... (数 4 2)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0 0 3 1】

なる秘密鍵  $(p, q, s, \beta)$  を作成し、さらに、

【0 0 3 2】

【数 4 3】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  ... (数 4 3)
- $n = p^d q \quad (d \text{ は奇数})$

【0 0 3 3】

なる公開鍵  $(n, g, h, k, l, \alpha)$  を作成し（但し、 $k$  は  $pq$  のビット長）。

【0 0 3 4】

[暗号化]

(1) 送信者は、平文  $m$  ( $0 < m < 2^{n-k-1}$ ) に対して、

【0 0 3 5】

【数 4 4】

$$m_1 = m0^{k_1} \oplus G(r) \parallel r \oplus H(m0^{k_1} \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \quad \dots \text{(数 4 4)}$$

【0 0 3 6】

を計算し（但し、 $G: \{0,1\}^{k_0} \rightarrow \{0,1\}^n$ ,  $H: \{0,1\}^n \rightarrow \{0,1\}^{k_0}$ , は適当なランダム関

数であり,  $k=n+k_0+2$ とする。), さらにJacobi記号 $a=(m_1/n)$ , および,

【0 0 3 7】

【数 4 5】

$$C = m_1^{2a} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \quad \dots (\text{数} 4 5)$$

【0 0 3 8】

を計算し,  $(C,D,a)$ を暗号文として受信者に送信する。

【0 0 3 9】

[復号化]

(2) 受信者は, 自身の秘密鍵  $(p,q,s,\beta)$  を用いて, 暗号文 $(C,D,a)$ から,

【0 0 4 0】

【数 4 6】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (\text{数} 4 6)$$

【0 0 4 1】

を計算し,  $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち,  $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を $m'_1$ として計算する。但し,  $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【0 0 4 2】

さらに,  $m'_1 = s' || t'$  ( $s'$ は $m'_1$ の上位 $n$ ビット,  $t'$ は下位 $k_0$ ビット)に対して,

【0 0 4 3】

【数 4 7】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \dots (\text{数} 4 7)$$

【0 0 4 4】

を計算し, これを復号化結果とする (但し,  $[a]^n$ および $[a]_n$ はそれぞれ $a$ の上位

および下位 $n$ ビットを表す。)

【0045】

【発明の実施の形態】

以下、図面を用いて、本発明の実施例について説明する。

【0046】

図1は、本発明の実施例のシステム構成を示す図である。このシステムは、送信者側装置100と受信者側装置200から構成されている。さらに、送信者側装置100と受信者側装置200は通信回線300で接続されている。

【0047】

図2は、実施例における送信者側装置100の内部構成を示す。送信者側装置100は、乱数生成手段101、べき乗算手段102、演算手段103、剰余演算手段104、メモリ105、通信装置106、を備えている。

【0048】

図3は、実施例における受信者側装置200の内部構成を示す。受信者側装置200は、鍵生成手段201、べき乗算手段202、剰余演算手段203、演算手段204、メモリ205、通信装置206、を備えている。

【0049】

図4は、実施例2の概要を示す図である。

【0050】

図5は、実施例3の概要を示す図である。

【0051】

図6は、実施例4の概要を示す図である。

【0052】

図7は、実施例5の概要を示す図である。

【0053】

図8は、本発明の実施例による方式と代表的な実用的公開鍵暗号方式との効率性（モジュラー積の個数）および安全性（IND-CCA2であるか）の比較を表す図である。図8における比較では、本発明の方式において $d=3$ とした。また、本発明の方式における括弧の中の数字は前処理が可能である場合において前処理を行っ

た結果である。

【 0 0 5 4 】

(実施例 1)

本発明の実施例として、まず、選択平文攻撃に対して一方向 (OW-CPA) であり、かつ選択平文攻撃に対して強秘匿 (IND-CPA) である公開鍵暗号方法について説明する。

【 0 0 5 5 】

鍵生成のステップとして、

【 0 0 5 6 】

【数 4 8】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  ... (数 4 8)

【 0 0 5 7 】

なる秘密鍵  $(p, q, s)$  を作成し、さらに、

【 0 0 5 8 】

【数 4 9】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$
- $n = p^d q \quad (d \text{ は奇数})$  ... (数 4 9)

【 0 0 5 9 】

なる公開鍵  $(n, g, h, k, l)$  を作成する (但し、 $k$  は  $pq$  のビット長)。

【 0 0 6 0 】

(1) 送信者は、平文  $m (0 < m < 2^{k-2})$  および乱数  $r (0 \leq r \leq 1)$  に対して、

【 0 0 6 1 】

【数 5 0】

$$C = m^2 g^r \bmod n, \quad D = h^r \bmod n \quad \dots \text{(数 5 0)}$$

【 0 0 6 2 】

を計算する，さらにJacobi記号 $a=(m/n)$ を計算し， $(C,D,a)$ を暗号文として前記受信者に送信する。

【 0 0 6 3 】

(2) 受信者は，自身の秘密鍵 $(p,q,s)$ を用いて，暗号文 $(C,D,a)$ から，

【 0 0 6 4 】

【数 5 1】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{(p+1)}{4}} \bmod p, & \dots (\text{数}51) \\ m_{1,q} &= (CD^s)^{\frac{(q+1)}{4}} \bmod q \end{aligned}$$

【 0 0 6 5 】

を計算し， $\phi(m_{1,p}, m_{1,q})$ ， $\phi(-m_{1,p}, m_{1,q})$ ， $\phi(m_{1,p}, -m_{1,q})$ ， $\phi(-m_{1,p}, -m_{1,q})$ のうち， $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を平文 $m$ とする（但し， $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。）。

【 0 0 6 6 】

~~この方法では，Jacobi記号 $a$ を暗号文の一部としており，これにより復号一意性が得られ，処理の高速化が可能となる。~~

【 0 0 6 7 】

上記公開鍵暗号方法をさらに選択暗号文攻撃に対して強秘匿（IND-CCA2）になるように変換したものを以下の各実施例にて示す。

【 0 0 6 8 】

(実施例 2)

本実施例は，メッセージの送信者であるAが受信者であるBに対して，送信データ $m$ を暗号通信によって送信する場合について説明する。

【 0 0 6 9 】

図 1 は，本実施例のシステム構成を示す。また，図 2 は，本実施例の概要を示す。

【 0 0 7 0 】

1. 鍵生成処理



受信者 B は、予め、受信者側装置 200 内の鍵生成手段 201 を用いて、

【 0 0 7 1 】

【数 5 2】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$        $\dots$  (数 5 2)

【 0 0 7 2 】

なる秘密情報  $(p, q, \beta)$  を作成し、

【 0 0 7 3 】

【数 5 3】

- $\alpha, k \in \mathbb{Z}$        $\dots$  (数 5 3)
- $n = p^d q$       ( $d$  は奇数)

【 0 0 7 4 】

なる公開情報  $(n, k, \alpha)$  を作成し（但し、 $k$  は  $p, q$  のビット長を表す。）、公開情報を通信回線 300 などを通して出力し、送信者側装置 100 へ送付するか、または公開する。公開する方法として、例えば第 3 者（公開情報管理機関）への登録など、周知の方法を用いることが可能である。その他の情報については、メモリ 205 に格納する。

【 0 0 7 5 】

## 2. 暗復号化处理

(1) 送信者 A は、平文  $m$  ( $0 < m < 2^{n-k_1}$ ) に対して、乱数生成手段 101、演算手段 103 を用いて、乱数  $r$  ( $0 < r < 2^{k_1}$ ) を選び、

【 0 0 7 6 】

【数 5 4】

$$m_1 = m0^{k_1} \oplus G(r) \parallel r \oplus H(m0^{k_1} \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \quad \dots \text{(数 5 4)}$$

【 0 0 7 7 】

を計算する。但し、 $G: \{0, 1\}^{k_0} \rightarrow \{0, 1\}^n$ ,  $H: \{0, 1\}^n \rightarrow \{0, 1\}^{k_0}$ , は適当なランダム

関数であり、 $k=n+k_0+2$ とする。

【0078】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103、べき乗算手段102、剰余演算手段104を用いて、Jacobi記号 $a=(m_1/n)$ 、および、

【0079】

【数55】

$$C = m_1^{2a} \bmod n,$$

・・・(数55)

【0080】

を計算する。

【0081】

さらに、暗号文 $(C, a)$ を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0082】

(2) 受信者Bは、保持している上記秘密情報 $(p, q, \beta)$ と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文 $(C, a)$ から

【0083】

【数56】

$$m_{1,p} = C^{\frac{\beta(p+1)}{4}} \bmod p,$$

$$m_{1,q} = C^{\frac{\beta(q+1)}{4}} \bmod q$$

・・・(数56)

【0084】

を計算し、 $\phi(m_{1,p}, m_{1,q})$ ,  $\phi(-m_{1,p}, m_{1,q})$ ,  $\phi(m_{1,p}, -m_{1,q})$ ,  $\phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を $m'_1$ として計算する。但し、 $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【0085】

さらに、演算手段204を用いて、 $m'_1 = s' || t'$  ( $s'$ は $m'_1$ の上位 $n$ ビット、 $t'$ は下

位 $k_0$ ビット) に対して,

【0 0 8 6】

【数 5 7】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \dots (\text{数 } 57)$$

【0 0 8 7】

を計算し, これを復号化結果とする (但し,  $[a]^n$  および  $[a]_n$  はそれぞれ  $a$  の上位および下位  $n$  ビットを表す。)

なお, 上記式において,  $m' = *$  とは, if 以下の条件が成立しないときは, 正しい復号結果が得られないものとしてエラーを出力する, あるいは復号化処理を中断するなど, システム構成に依存する処理を行うことを示している。

【0 0 8 8】

上記方法を用いれば, 適応的選択暗号文攻撃に対して強秘匿であることが  $n$  の素因数分解問題の困難性との等価性により証明することができる。

【0 0 8 9】

また, 本実施例の方法によると, 暗号化処理はほぼ 2 回のモジュラー積を行うのみであり, また, 復号化処理においては  $n$  よりも小さい  $pq$  の上で行うことにより, 従来方法に比べて処理の高速性を実現している。

【0 0 9 0】

(実施例 3)

本実施例は, 実施例 1 が決定的アルゴリズム (確率暗号ではない) から IND-CC A2 となるように変換したものであるのに対して, 確率的アルゴリズムから IND-CC A2 になるように変換したものである。

【0 0 9 1】

## 1. 鍵生成処理

受信者 B は, 予め, 受信者側装置 200 内の鍵生成手段 201 を用いて,

【 0 0 9 2 】

【数 5 8】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  . . . (数 5 8)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【 0 0 9 3 】

なる秘密情報  $(p, q, s, \beta)$  を作成し,

【 0 0 9 4 】

【数 5 9】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  . . . (数 5 9)
- $n = p^d q \quad (d \text{ は奇数})$

【 0 0 9 5 】

なる公開情報  $(n, g, h, k, l, \alpha)$  を作成し (但し,  $k$  は  $p, q$  のビット長を表す。) , 公開情報を通信回線 300 などを介して出力し, 送信者側装置 100 へ送付するか, または公開する。公開する方法として, 例えば第 3 者 (公開情報管理機関) への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ 205 に格納する。

【 0 0 9 6 】

2. 暗復号化处理

(1) 送信者 A は, 平文  $m$  ( $0 < m < 2^{n-k_1}$ ) に対して, 乱数生成手段 101, 演算手段 103 を用いて, 乱数  $r$  ( $0 < r < 2^{k_1}$ ) を選び,

【 0 0 9 7 】

【数 6 0】

$$m_1 = m0^{k_1} \oplus G(r) \parallel r \oplus H(m0^{k_1} \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \quad \dots \text{(数 6 0)}$$

【 0 0 9 8 】

を計算する。但し、 $G: \{0,1\}^{k_0} \rightarrow \{0,1\}^n$ ,  $H: \{0,1\}^n \rightarrow \{0,1\}^{k_0}$ , は適当なランダム関数であり、 $k=n+k_0+2$ とする。

【 0 0 9 9 】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103, べき乗算手段102, 剰余演算手段104を用いて、Jacobi記号 $a=(m_1/n)$ , および、

【 0 1 0 0 】

【数 6 1】

$$C = m_1^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \quad \dots (数61)$$

【 0 1 0 1 】

を計算する。

【 0 1 0 2 】

さらに、暗号文  $(C,D,a)$  を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 1 0 3 】

(2) 受信者Bは、保持している上記秘密情報  $(p,q,s,\beta)$  と、受信者側装置200内のべき乗算手段202, 剰余演算手段203, 演算手段204を用いて暗号文  $(C,D,a)$  から、

【 0 1 0 4 】

【数 6 2】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (数62)$$

【 0 1 0 5 】

を計算し、 $\phi(m_{1,p}, m_{1,q})$ ,  $\phi(-m_{1,p}, m_{1,q})$ ,  $\phi(m_{1,p}, -m_{1,q})$ ,  $\phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を $m'_1$ として計算する。但し、 $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【0 1 0 6】

さらに、演算手段204を用いて、 $m'_1 = s' || t'$  ( $s'$  は  $m'_1$  の上位  $n$  ビット、 $t'$  は下位  $k_0$  ビット) に対して、

【0 1 0 7】

【数 6 3】

$$m' = \begin{cases} [s' \oplus G(t' \oplus H(s'))]^{n-k_1} & \text{if } [s' \oplus G(t' \oplus H(s'))]_{k_1} = 0^{k_1} \\ * & \text{otherwise} \end{cases} \quad \dots \text{(数 6 3)}$$

【0 1 0 8】

を計算し、これを復号化結果とする（但し、 $[a]^n$  および  $[a]_n$  はそれぞれ  $a$  の上位および下位  $n$  ビットを表す。）

本実施例による方法では、 $n$  の素因数分解問題よりも困難な問題の困難性を前提として、IND-CCA2であることを示すことができる。

【0 1 0 9】

(実施例 4)

上記実施例 3 において、

【0 1 1 0】

【数 6 4】

$$g^{r'} \bmod n, \quad h^{r'} \bmod n \quad \dots \text{(数 6 4)}$$

【0 1 1 1】

の計算は、暗号化対象である送信データ  $m$  に関係しないため、前処理が可能である。すなわち、これらの計算を前処理として行い、その結果をコンピュータ A の記憶手段（メモリ、二次記憶装置など）に保存して、その値を読み出して用いることにより、暗号化時間を大幅に短縮する事ができる。

【0 1 1 2】

前処理を行うと、送信データ  $m$  を用いた処理のモジュラー積の個数は 1 個となるため、暗号化時間を大幅に短縮することが可能となる。

【0 1 1 3】

(実施例 5)

本実施例は、実施例 3 の変形例である。

【0 1 1 4】

## 1. 鍵生成処理

受信者 B は、予め、受信者側装置 200 内の鍵生成手段 201 を用いて、

【0 1 1 5】

【数 6 5】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  ... (数 6 5)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0 1 1 6】

なる秘密情報  $(p, q, s, \beta)$  を作成し、

【0 1 1 7】

【数 6 6】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  ... (数 6 6)
- $n = p^d q \quad (d \text{ は奇数})$

【0 1 1 8】

なる公開情報  $(n, g, h, k, l, \alpha)$  を作成し (但し,  $k$  は  $p, q$  のビット長を表す。), 公開情報を通信回線 300 などを介して出力し, 送信者側装置 100 へ送付するか, または公開する。公開する方法として, 例えば第 3 者 (公開情報管理機関) への登録など, 周知の方法を用いることが可能である。その他の情報については, メモリ 205 に格納する。

【0 1 1 9】

## 2. 暗復号化処理

(1) 送信者 A は, 平文  $m$  ( $0 < m < 2^n$ ) に対して, 乱数生成手段 101, 演算手段 103

を用いて、乱数 $r$  ( $0 < r < 2^{k_0}$ ) を選び、

【 0 1 2 0 】

【数 6 7】

$$m_1 = m \oplus G(r) \parallel r \oplus H(m \oplus G(r)) \quad (0 < m_1 < 2^{k-2}) \quad \dots (数67)$$

【 0 1 2 1 】

を計算する。但し、 $G: \{0,1\}^{k_0} \rightarrow \{0,1\}^n$ ,  $H: \{0,1\}^n \rightarrow \{0,1\}^{k_0}$ , は適当なランダム関数であり、 $k=n+k_0+2$ とする。

【 0 1 2 2 】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103、べき乗算手段102、剰余演算手段104を用いて、Jacobi記号 $a=(m_1/n)$ , および、

【 0 1 2 3 】

【数 6 8】

$$C = m_1^{2a} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \quad \dots (数68)$$

【 0 1 2 4 】

を計算する。但し、 $F: \{0,1\}^{n+k_0} \rightarrow \{0,1\}^1$  は適当なランダム関数。

【 0 1 2 5 】

さらに、暗号文  $(C,D,a)$  を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 1 2 6 】

(2) 受信者Bは、保持している上記秘密情報  $(p,q,s,\beta)$  と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文  $(C,D,a)$  から、

【 0 1 2 7 】

【数 6 9】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (数69)$$



【0 1 2 8】

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を $m'_1$ として計算する。但し、 $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【0 1 2 9】

さらに、演算手段204を用いて、 $m'_1 = s' || t'$  ( $s'$ は $m'_1$ の上位 $n$ ビット、 $t'$ は下位 $k_0$ ビット) に対して、

【0 1 3 0】

【数 7 0】

$$m' = \begin{cases} s' \oplus G(t' \oplus H(s')) & \text{if } (C, D) = (C', D') \\ * & \text{otherwise} \end{cases} \quad \dots (\text{数 } 70)$$

【0 1 3 1】

を計算し、これを復号化結果とする。但し、

【0 1 3 2】

【数 7 1】

$$C' = m_1'^2 g^{F(m_1')} \bmod n, \quad D' = h^{F(m_1')} \bmod n \quad \dots (\text{数 } 71)$$

【0 1 3 3】

であり、 $[a]^n$ および $[a]_n$ はそれぞれ $a$ の上位および下位 $n$ ビットを表す。

【0 1 3 4】

本実施例による方法では、 $n$ の素因数分解問題よりも困難な問題の困難性を前提として、IND-CCA2であることを示すことができる。

【0 1 3 5】

また、本実施例の方法においては、実施例3の方法に比べて、平文を長くとることが可能である。

【0 1 3 6】

(実施例 6)

本実施例は、実施例3の変形例である。

【 0 1 3 7 】

## 1. 鍵生成処理

受信者 B は、予め、受信者側装置 200 内の鍵生成手段 201 を用いて、

【 0 1 3 8 】

【数 7 2】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  ... (数 7 2)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【 0 1 3 9 】

なる秘密情報  $(p, q, s, \beta)$  を作成し、

【 0 1 4 0 】

【数 7 3】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  ... (数 7 3)
- $n = p^d q \quad (d \text{ は奇数})$

【 0 1 4 1 】

なる公開情報  $(n, g, h, k, l, \alpha)$  を作成し（但し、 $k$  は  $p, q$  のビット長を表す。）  
 , 公開情報を通信回線 300 などを介して出力し、送信者側装置 100 へ送付するか、  
 または公開する。公開する方法として、例えば第 3 者（公開情報管理機関）への  
 登録など、周知の方法を用いることが可能である。その他の情報については、メ  
 モリ 205 に格納する。

【 0 1 4 2 】

## 2. 暗復号化処理

(1) 送信者 A は、平文  $m$  ( $0 < m < 2^n$ ) に対して、乱数生成手段 101、演算手段 103  
 を用いて、乱数  $r$  ( $0 < r < 2^{k_0}$ ) を選び、

【 0 1 4 3 】

【数 7 4】

$$m_1 = m \parallel r$$

・・・(数74)

【 0 1 4 4 】

を計算する。但し、 $F: \{0,1\}^{n+k_0} \rightarrow \{0,1\}^l$  は適当なランダム関数であり、 $k=n+k_0+2$ とする。

【 0 1 4 5 】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103、べき乗算手段102、剰余演算手段104を用いて、Jacobi記号 $a=(m_1/n)$ 、および、

【 0 1 4 6 】

【数 7 5】

$$C = m_1^{2\alpha} g^{F(m_1)} \bmod n, \quad D = h^{F(m_1)} \bmod n \quad \cdots \text{(数75)}$$

【 0 1 4 7 】

を計算する。

【 0 1 4 8 】

さらに、暗号文 $(C,D,a)$ を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【 0 1 4 9 】

(2) 受信者Bは、保持している上記秘密情報 $(p,q,s,\beta)$ と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文 $(C,D,a)$ から、

【 0 1 5 0 】

【数 7 6】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (\text{数 } 76)$$

【 0 1 5 1 】

を計算し、 $\phi(m_{1,p}, m_{1,q})$ ,  $\phi(-m_{1,p}, m_{1,q})$ ,  $\phi(m_{1,p}, -m_{1,q})$ ,  $\phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を $m'_1$ として計算する。但し、 $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【 0 1 5 2 】

さらに、演算手段204を用いて、

【 0 1 5 3 】

【数 7 7】

$$m' = \begin{cases} [m'_1]^{k_0} & \text{if } (C, D) = (C', D') \\ * & \text{otherwise} \end{cases} \quad \dots (\text{数 } 77)$$

【 0 1 5 4 】

を計算し、これを復号化結果とする。但し、

【 0 1 5 5 】

【数 7 8】

$$C' = m_1'^{2\alpha} g^{F(m'_1)} \bmod n, \quad D' = h^{F(m'_1)} \bmod n \quad \dots (\text{数 } 78)$$

【 0 1 5 6 】

であり、 $[a]^n$ および $[a]_n$ はそれぞれ $a$ の上位および下位 $n$ ビットを表す。

【 0 1 5 7 】

本実施例による方法では、「条件付きDiffie-Hellman問題」の困難性を前提として、IND-CCA2であることを示すことができる。

【0 1 5 8】

また、本実施例の方法においては、実施例 3 の方法に比べて、平文を長くとることが可能である。

【0 1 5 9】

(実施例 7)

本実施例は、実施例 5 および実施例 6 において、受信者側の計算効率を高めるための復号化方法について述べる。

【0 1 6 0】

受信者は、受信者側装置 200 内のべき乗算手段 202、剰余演算手段 203、演算手段 204 を用いて、

【0 1 6 1】

【数 7 9】

$$\begin{aligned} C'_p &= m_1'^{2\alpha} g^{F(m'_1)} \bmod p^d, & C'_q &= m_1'^{2\alpha} g^{F(m'_1)} \bmod q \\ D'_p &= h^{F(m'_1)} \bmod p^d, & D'_q &= h^{F(m'_1)} \bmod q \end{aligned} \quad \dots (\text{数 } 79)$$

【0 1 6 2】

を計算し、さらに

【0 1 6 3】

【数 8 0】

$$\begin{aligned} C &\equiv C'_p \pmod{p^d}, & C &\equiv C'_q \pmod{q}, \\ D &\equiv D'_p \pmod{p^d}, & D &\equiv D'_q \pmod{q} \end{aligned} \quad \dots (\text{数 } 80)$$

【0 1 6 4】

により、 $(C, D) = (C', D')$  を検査する。

【0 1 6 5】

(実施例 8)

本実施例は、選択平文攻撃に対して強秘匿、すなわち IND-CPA、である公開鍵暗号方法について述べる。

【0 1 6 6】

# 1. 鍵生成処理

受信者 B は、予め、受信者側装置 200 内の鍵生成手段 201 を用いて、

【0 1 6 7】

【数 8 1】

- $p, q$  : 素数,  $p \equiv 3 \pmod{4}, q \equiv 3 \pmod{4}$
- $s \in \mathbb{Z}, gh^s \equiv 1 \pmod{pq}$  . . . (数 8 1)
- $\beta \in \mathbb{Z}, \alpha\beta \equiv 1 \pmod{\text{lcm}(p-1, q-1)}$

【0 1 6 8】

なる秘密情報  $(p, q, s, \beta)$  を作成し、

【0 1 6 9】

【数 8 2】

- $\alpha, g, h, k, l \in \mathbb{Z} \quad (0 < g, h < n)$  . . . (数 8 2)
- $n = p^d q \quad (d \text{ は奇数})$

【0 1 7 0】

なる公開情報  $(n, g, h, k, l, \alpha)$  を作成し（但し、 $k$  は  $p, q$  のビット長を表す。）  
、公開情報を通信回線 300 などを通して出力し、送信者側装置 100 へ送付するか、  
または公開する。公開する方法として、例えば第 3 者（公開情報管理機関）への  
登録など、周知の方法を用いることが可能である。その他の情報については、メ  
モリ 205 に格納する。

【0 1 7 1】

# 2. 暗復号化処理

(1) 送信者 A は、平文  $m$  ( $0 < m < 2^{k-2}$ ) に対して、乱数生成手段 101、演算手段 10  
3 を用いて、乱数  $r$  ( $0 < r < l$ ) を選び、

【0 1 7 2】

【数 8 3】

$$C = m^{2\alpha} g^{r'} \bmod n, \quad D = h^{r'} \bmod n \quad \dots (数 8 3)$$

【0 1 7 3】

を計算する。

【0 1 7 4】

さらに、第3者あるいは受信者Bから上記公開情報を得て、演算手段103、べき乗算手段102、剰余演算手段104を用いて、Jacobi記号 $a=(m/n)$ を計算する。

【0 1 7 5】

さらに、暗号文 $(C,D,a)$ を通信装置106を用いて通信回線300を介して受信者Bの受信者側装置200に送信する。

【0 1 7 6】

(2) 受信者Bは、保持している上記秘密情報 $(p,q,s,\beta)$ と、受信者側装置200内のべき乗算手段202、剰余演算手段203、演算手段204を用いて暗号文 $(C,D,a)$ から、

【0 1 7 7】

【数 8 4】

$$\begin{aligned} m_{1,p} &= (CD^s)^{\frac{\beta(p+1)}{4}} \bmod p, \\ m_{1,q} &= (CD^s)^{\frac{\beta(q+1)}{4}} \bmod q \end{aligned} \quad \dots (数 8 4)$$

【0 1 7 8】

を計算し、 $\phi(m_{1,p}, m_{1,q}), \phi(-m_{1,p}, m_{1,q}), \phi(m_{1,p}, -m_{1,q}), \phi(-m_{1,p}, -m_{1,q})$ のうち、 $(x/n)=a$ かつ $0 < x < 2^{k-2}$ を満たす $x$ を平文 $m$ として計算する。但し、 $\phi$ は中国人の剰余定理による $Z/(p) \times Z/(q)$ から $Z/(pq)$ への環同型写像を表す。

【0 1 7 9】

本実施例による方法では、 $n$ の素因数分解問題よりも困難な問題の困難性を前

提として完全解読が不可能なこと、さらに「条件付きのDiffie-Hellman決定問題」の困難性を前提として強秘匿であることを示すことができる。ここで、「条件付きのDiffie-Hellman決定問題」とは、確率分布

【0 1 8 0】

【数 8 5】

$$\begin{aligned} D_0 &: (h, g, h^r, g^r), \quad 0 \leq r \leq l, \\ D_1 &: (h, g, h^r, Xg^r), \quad X = (x/x')^{2\alpha} \bmod n, \quad 0 < x, x' < 2^{k-2} \end{aligned} \quad \cdots (\text{数} 85)$$

【0 1 8 1】

において、 $D_0$  または  $D_1$  からの任意のシーケンスに対して、いずれからのものであるかを言い当てる問題である。

【0 1 8 2】

以上、実施例では、送信者と受信者が各々の装置を利用して暗号通信を行うという一般形で述べたが、具体的には様々なシステムに適用される。

【0 1 8 3】

例えば、電子ショッピングシステムでは、送信者はユーザであり、送信者側装置はパソコンなどの計算機であり、受信者は小売店、受信者側装置はパソコンなどの計算機となる。このとき、ユーザの商品等の注文書は共通鍵暗号で暗号化されることが多く、その際の暗号化鍵を本実施例による方法により暗号化されて小売店側装置に送信される。

【0 1 8 4】

また、電子メールシステムでは、各々の装置はパソコンなどの計算機であり、送信者のメッセージは共通鍵暗号で暗号化されることが多く、その際の暗号化鍵を本実施例による方法により暗号化されて受信者の計算機に送信される。

【0 1 8 5】

その他にも、従来の公開鍵暗号が使われている様々なシステムに適用することが可能である。



【 0 1 8 6 】

なお、本実施例における各計算は、CPUがメモリ内の各プログラムを実行することにより行われるものとして説明したが、プログラムだけではなく、いずれかがハードウェア化された演算装置であって、他の演算装置や、CPUと、データのやりとりを行うものであっても良い。

【 0 1 8 7 】

【発明の効果】

本発明によれば、最も強力な攻撃法である適応的選択暗号文攻撃に対しても安全であり、さらに、高速処理が可能な、公開鍵暗号方法と、その応用装置、システムを実現することができる。

【図面の簡単な説明】

【図 1】

本発明の実施例のシステム構成を示す図である。

【図 2】

本発明の実施例における送信者側装置の内部構成を示す図である。

【図 3】

本発明の実施例における受信者側装置の内部構成を示す図である。

【図 4】

本発明の実施例 2 の概要を示す図である。

【図 5】

本発明の実施例 3 の概要を示す図である。

【図 6】

本発明の実施例 4 の概要を示す図である。

【図 7】

本発明の実施例 5 の概要を示す図である。

【図 8】

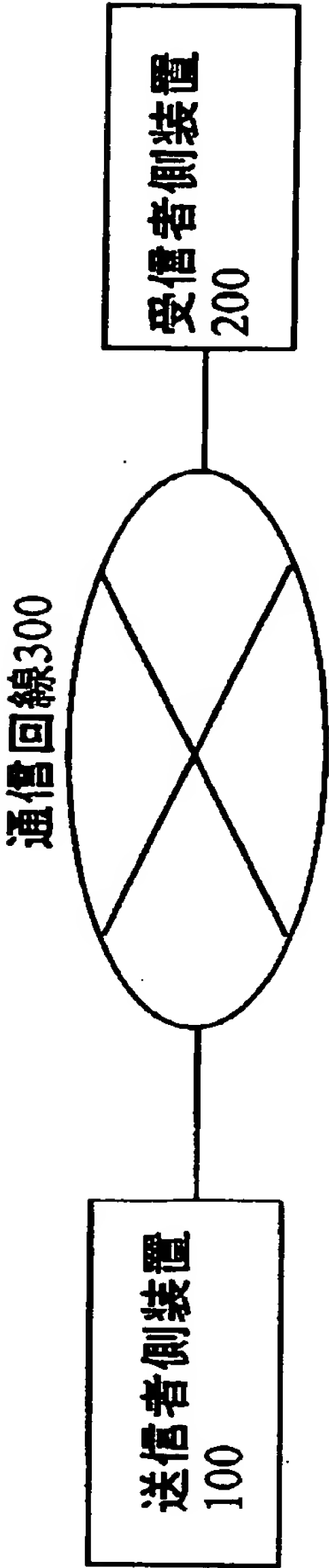
本発明の実施例による方式と代表的な実用的公開鍵暗号方式との効率性（モジュラー積の個数）の比較を表す図である。

## 【符号の説明】

1 0 0 …送信者側装置, 1 0 1 …送信者側装置 1 0 0 内の乱数生成手段, 1 0 2 …送信者側装置 1 0 0 内のべき乗算手段, 1 0 3 …送信者側装置 1 0 0 内の演算手段, 1 0 4 …送信者側装置 1 0 0 内の剰余演算手段, 1 0 5 …送信者側装置 1 0 0 内のメモリ, 1 0 6 …送信者側装置 1 0 0 内の通信装置, 2 0 0 …受信者側装置, 2 0 1 …受信者側装置 2 0 0 内の鍵生成手段, 2 0 2 …受信者側装置 2 0 0 内のべき乗算手段, 2 0 3 …受信者側装置 2 0 0 内の剰余演算手段, 2 0 4 …受信者側装置 2 0 0 内の演算手段, 2 0 5 …受信者側装置 2 0 0 内のメモリ, 2 0 6 …受信者側装置 2 0 0 内の通信装置。。

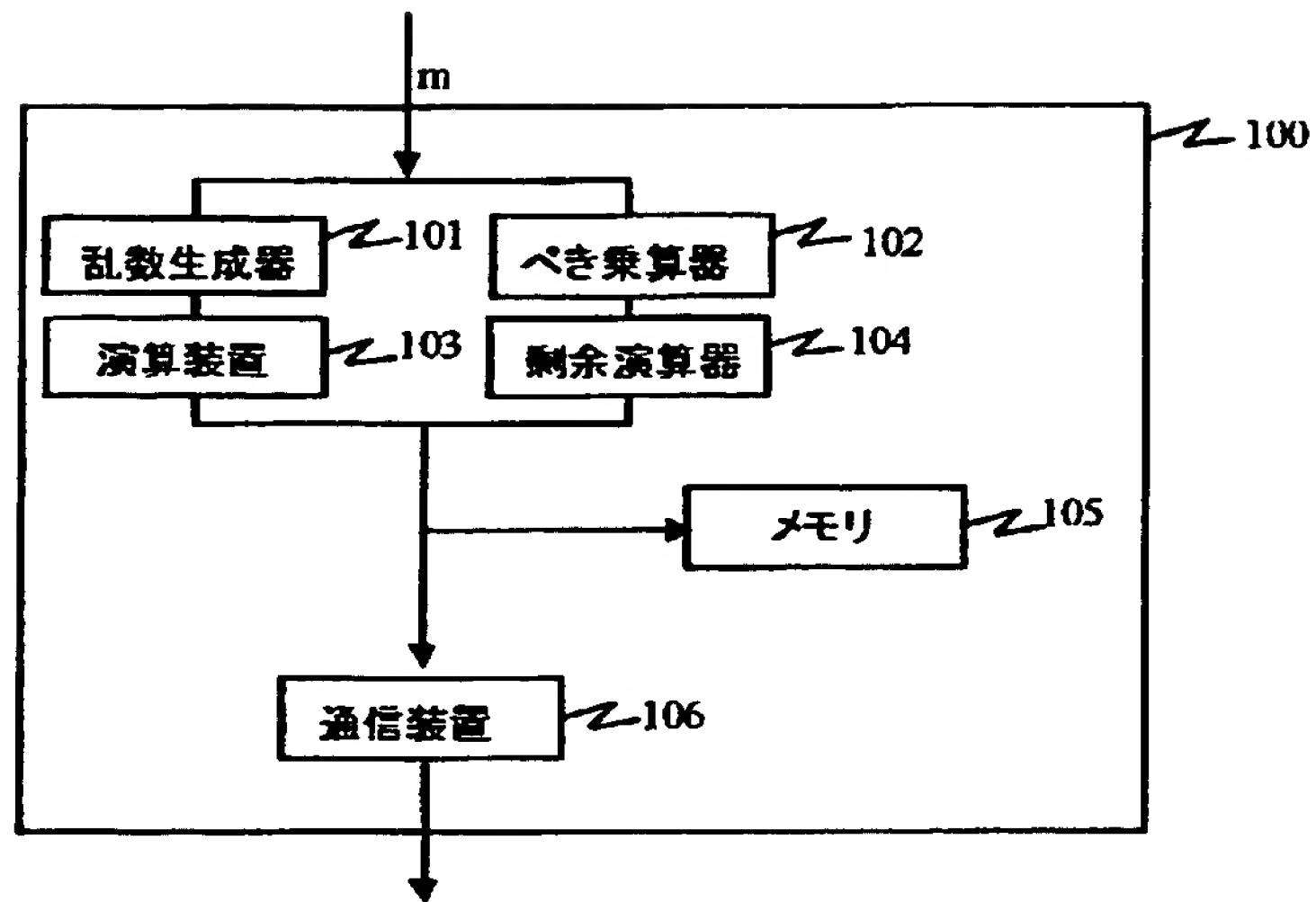
【書類名】 図面  
【図 1】

図 1



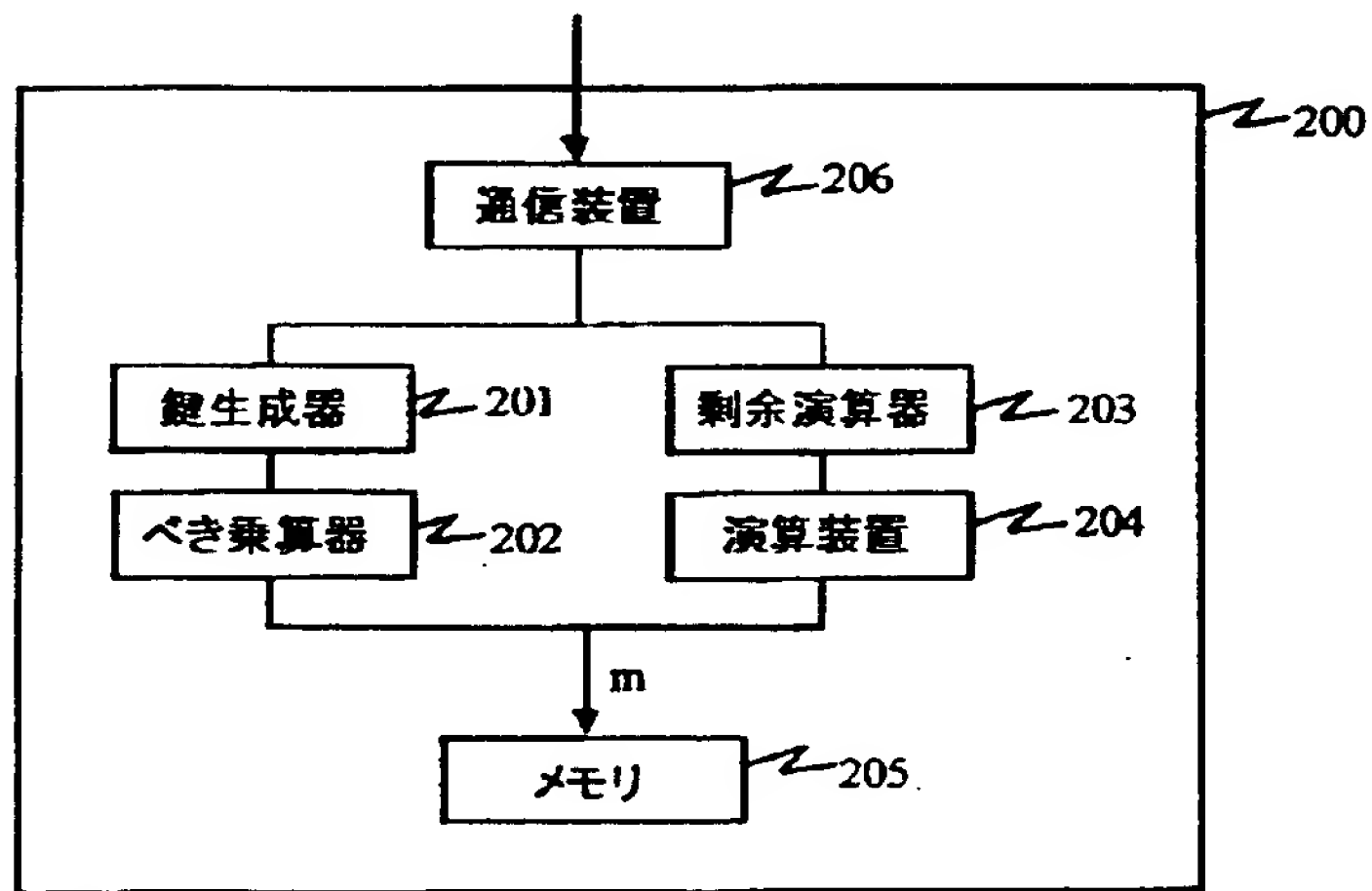
【図 2】

図 2



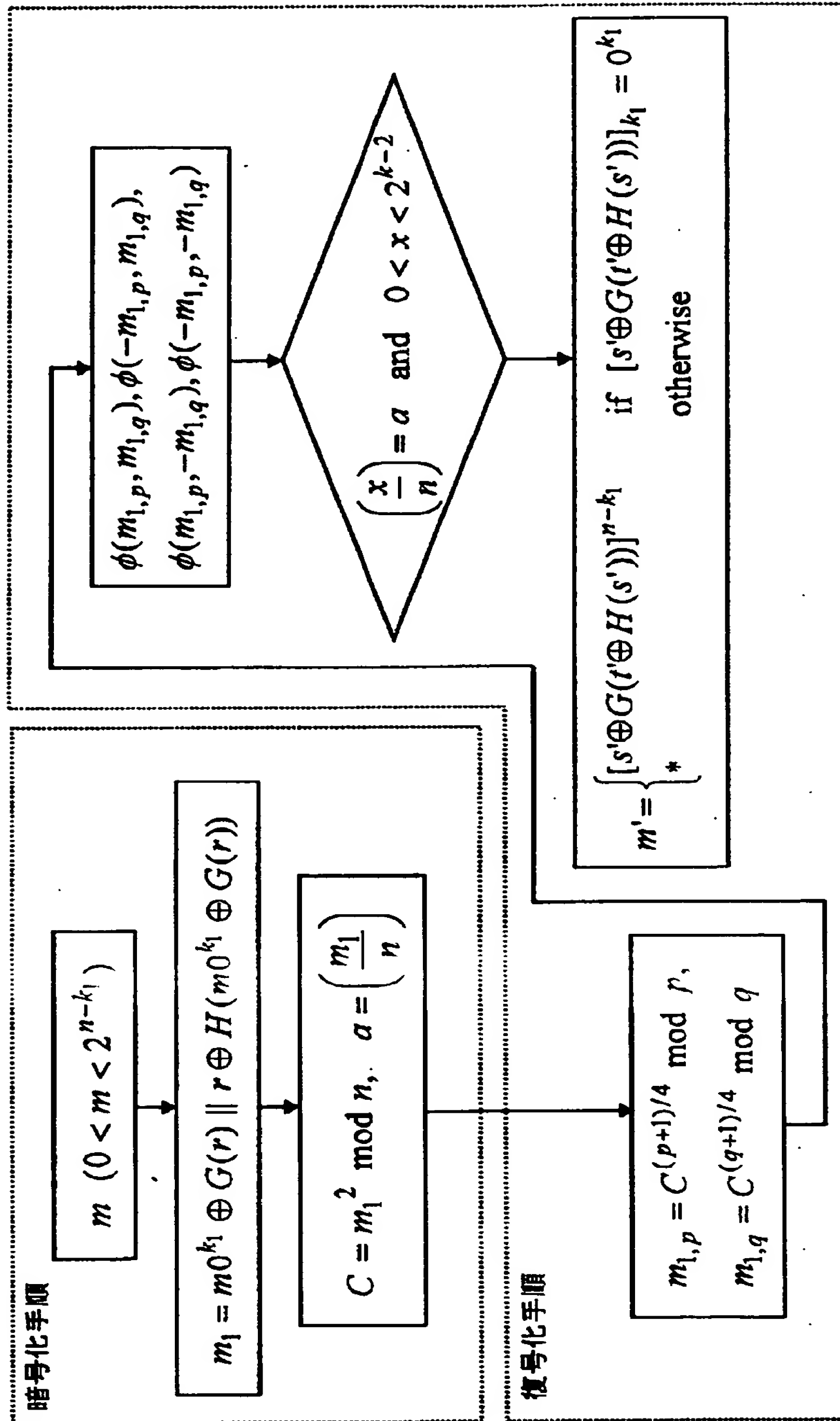
【図 3】

図 3

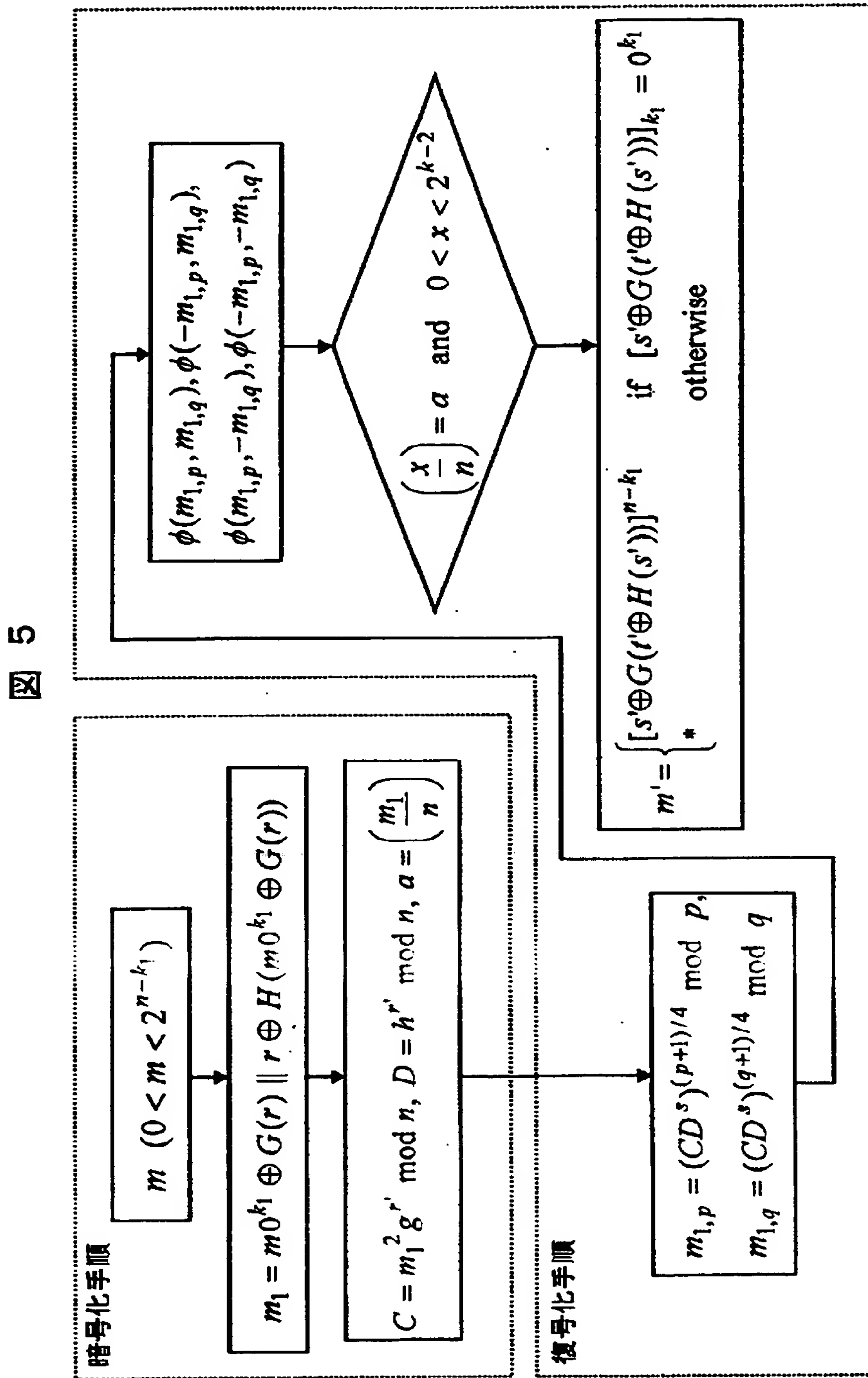


【図 4】

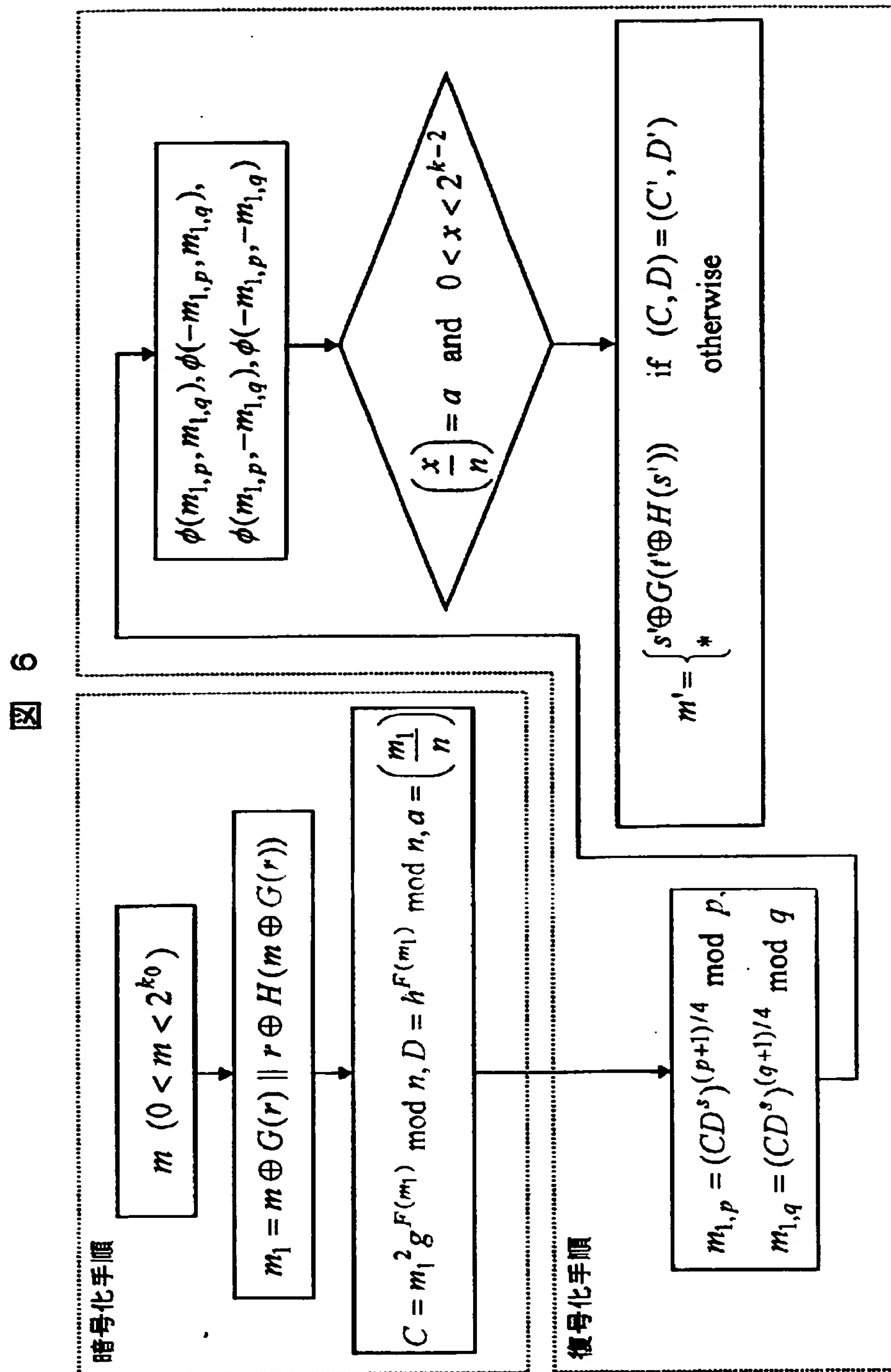
図 4



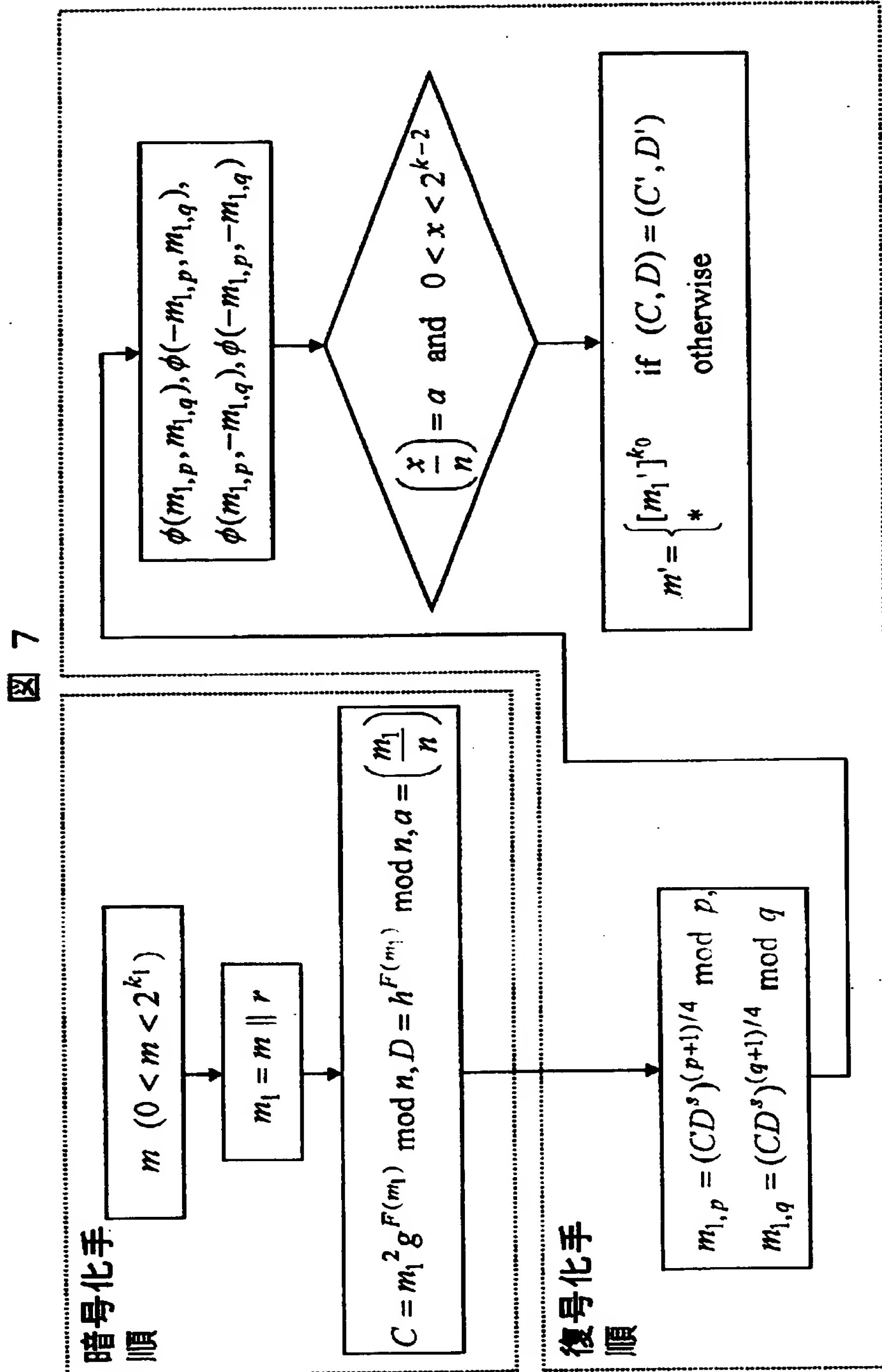
【図 5】



【図 6】



【図 7】





【図 8】

図 8

	暗号化	復号化	IND-CCA2
RSA	約 2~1500	約 400	No
ElGamal暗号	約 3000	約 1500	No
楕円暗号	約 120	約 60	No
OAEP	約 2~1500	約 400	Yes
本発明の方式	約 2~200	約 60~210	Yes

【書類名】 要約書

【要約】

【課題】

受信者の公開鍵を用いて、送信データを暗号化する公開鍵暗号による暗号通信方法であって、適応的暗号文攻撃に対して強秘匿であることの証明により安全性を保証することができ、かつ、暗復号化のための計算において効率性の高い処理ができる公開鍵暗号方法および装置を提供する。

【解決手段】

選択平文攻撃に対する一方向性（OW-CPA）を素因数分解問題よりも困難な問題の難しさを前提として保証可能な公開鍵暗号方法に対して、平文に乱数情報と（理想的）ランダム関数へのアクセスの結果から排他的論理和および接続（データの単純な接続）の変換（以下、変換Conと呼ぶ）を行うことにより、適応的選択暗号文攻撃に対する強秘匿性（IND-CCA2）を、素因数分解問題の困難性以上の暗号学的仮定により保証する。

【選択図】 図 1

出 願 人 履 歴 情 報

識別番号 [ 0 0 0 0 0 5 1 0 8 ]

1. 変更年月日 1 9 9 0 年 8 月 3 1 日

[ 変更理由 ] 新規登録

住 所 東京都千代田区神田駿河台 4 丁目 6 番地

氏 名 株式会社日立製作所



1

1

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

**BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**

**This Page Blank (uspto)**